Inspector General
United States Department of Defense

Hotline Review June 28, 2011

Hotline Complaint Regarding a Defense Contract Audit Agency Employee Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment

Report No. D-2011-6-008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
28 JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Hotline Complaint Regarding A Defense Contract Audit Agency Employee Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Inspector General,400 Army Navy Drive,Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

Additional Information

The Department of Defense Office of the Deputy Inspector General for Policy and Oversight, Audit Policy and Oversight, prepared this report. If you have questions, contact the signer of the report.

Suggestions for Future Reviews

To suggest ideas for or to request future reviews, contact the Office of the Assistant Inspector General for Audit Policy and Oversight at (703) 604-8760 (DSN 664-8760) or fax (703) 604-8982. Ideas and requests can also be mailed to:

Office of the Assistant Inspector General
for Audit Policy and Oversight
Department of Defense Inspector General
400 Army Navy Drive (Room 833)
Arlington, VA 22202-4704

Acronyms and Abbreviations

DCAA	Defense Contract Audit Agency
GAO	Government Accountability Office
OMB	Office of Management and Budget
PII	Personally Identifiable Information

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

JUN 28 2011

MEMORANDUM FOR DIRECTOR, DEFENSE CONTRACT AUDIT AGENCY

SUBJECT: Hotline Complaint Regarding A Defense Contract Audit Agency Employee Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment (Report No. D-2011-6-008)

We are providing this report for your information and use. We reviewed a Defense Hotline complaint and substantiated the allegation that a Defense Contract Audit Agency employee was conducting private for-profit tax business activities on Government time and using Government equipment. During our review, we also found unauthorized personally identifiable information and unauthorized software on the employee's Government-issued computer.

We considered management comments on a draft of this report when preparing the final report. The comments conformed to the requirements of DOD Directive 7650.3 and left no unresolved issues. Therefore, additional comments are not required.

We appreciate the courtesies extended to the staff. Please direct questions to Ms. Carolyn R. Davis at (703) 604-8877 (DSN 664-8877).

Randolph R. Stone, SES
Deputy Inspector General
for Policy and Oversight

Results in Brief: Hotline Complaint Regarding A Defense Contract Audit Agency Employee Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment

What We Did

We reviewed the DOD Hotline complaint alleging that a Defense Contract Audit Agency (DCAA) employee conducted private for-profit tax business activity on Government time and using Government equipment.

What We Found

We substantiated the allegation. We found that the employee was conducting activities associated with his private for-profit tax business on Government time and using Government equipment. During our review, we also found:

- unauthorized personally identifiable information on the subject's Government computer; and
- unauthorized software on the subject's Government computer.

What We Recommend

We recommend that the Director, Defense Contract Audit Agency:

- Take appropriate action against the employee for ethics breaches, and determine how to mitigate the risk vulnerability of auditors that have private businesses from performing private business tasks on Government time while teleworking.
- Contact the U.S. Department of the Treasury, the specific State Board of Public Accountancy, and the American Institute of Certified Public Accountants to determine whether any Federal or State laws, regulations, policies, or rules were broken.
- Determine how to mitigate the risk of unauthorized personally identifiable information from entering the information systems network.

Management Comments and Our Response

In responding to an April 11, 2011 draft of this report, the Director, DCAA agreed with all findings and recommendations. Therefore, no further comments are required.

United States Department of Defense
Office of Inspector General
Project No. D2010-DIP0AI-0253.000
Report No. D-2011-6-008
June 28, 2011

Table of Contents

Introduction

Objectives

We conducted this review to determine whether the complainant's allegation concerning an employee conducting private for-profit tax business activity on Government time and using Government equipment could be substantiated. The complainant, who is anonymous, specifically alleged that:

- the employee was regularly heard talking to clients on the phone; and
- the employee was using a Government fax machine to send and receive client documents.

See Appendix for details regarding our scope and methodology.

Background

Defense Contract Audit Agency (DCAA)

DCAA is a Defense agency under the authority, direction, and control of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense. In accordance with DOD Directive 5105.36, DCAA is responsible for performing contract audits for DOD, and providing accounting and financial advisory services regarding contracts and subcontracts to all DOD Components responsible for procurement and contract administration. These services are provided in connection with negotiation, administration, and settlement of contracts and subcontracts. In addition, DCAA also provides contract audit services to other Federal agencies, as appropriate.

Organizationally, DCAA includes a Headquarters, a Field Detachment, and five regions: Central, Eastern, Mid-Atlantic, Northeastern, and Western. Each region has several field audit offices. DCAA consists of approximately 4,800 people located at more than 300 field audit offices throughout the United States, Europe and the Pacific.

DCAA Internal Review Team

The DCAA Internal Review Team is responsible for investigating allegations of wrongdoing made against agency employees. The Internal Review Team received the complaint addressed in this report and forwarded it to us for action because of a possible perceived independence concern.

Finding A. Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment

We substantiated the allegation in the DOD Hotline complaint that a DCAA employee was conducting private for-profit tax business activity on Government time and using Government equipment by:

- seizing the computer of the subject of the complaint and analyzing its contents;
- interviewing and recording the subject of the complaint under oath; and
- applying applicable laws, policies, and regulations to this situation.

DCAA Ethics Policy

Ethics policies within the Executive branch of the Federal Government directs the use of Government time and property for authorized purposes only. DCAA follows and does not further supplement DOD's ethics policies. DOD ethics policies are contained in DOD 5500.7-R, Joint Ethics Regulation (JER), August 1, 1993 [with changes 1-6, dated March 23, 2006]. Chapter 2 of the Joint Ethics Regulation which supplements 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch, prohibits the use of Government time and property except for authorized Government purposes. Although neither of these references provide, as an example, the specific strict prohibition of performing tasks associated with a private for-profit business on Government time and using Government property, the DOD's Office of General Counsel Encyclopedia of Ethical Failure, dated July 2010, lists numerous examples where Federal employees have been punished for doing so.

DCAA Policy on Conducting Private For-Profit Business Activities on Government Equipment

DCAA policy does not permit employees to conduct private for-profit business activities on Government equipment. DCAA Regulations No. 4140.2, Use of Government Office Equipment, dated September 13, 2002, and No. 8500.1, Information Assurance (IA) Program, dated September 24, 2009, both strictly prohibit the use of Government equipment to maintain or support a personal private for-profit business or activity.

Analysis of Content on the Subject's Government-Issued Computer

We substantiated the allegation through our analysis of the subject's Government-issued computer. We seized the subject's Government-issued computer and our analysis

revealed 149 documents associated with the subject's private for-profit tax business. These documents were in the form of:

- 107 e-mails (many having attachments),
- 27 Adobe PDF documents,
- 12 Microsoft Excel documents, and
- 3 Microsoft Word documents.

Interview of the Subject

We further substantiated the allegation by performing an in-person interview with the subject of the complaint. Throughout the interview, the subject admitted to performing tasks associated with his private for-profit tax business on Government time and using Government equipment. During the interview, the subject confirmed the following:

- He was a Certified Public Accountant and licensed to practice.
- The name of the company, e-mail address and telephone number used in his private for-profit tax business.
- A listing of 29 names of individuals or companies obtained from the subject's Government computer, and whether or not they were clients of his private for-profit tax business.
- Certifications of annual training in ethics, privacy, and information assurance (authorized Government computer use).
- A selection of the 149 documents pertaining to the subject's private for-profit tax business found on his Government computer.

Subject's Sworn Statement Concerning His Private For-Profit Tax Business Activities on Government Time and Equipment

During our interview of the subject, he acknowledged using Government time and equipment to perform tasks associated with his private for-profit tax business. The subject also acknowledged his electronically-signed annual ethics and information assurance training documents, and admitted to knowing that it was improper to use Government time and equipment to perform tasks associated with a private for-profit business.

DCAA Risk Vulnerability

A risk vulnerability exists within DCAA for auditors that have private for-profit businesses and telework to perform tasks associated with their private businesses on Government time. Although teleworking did not cause the situation being reported here, since the employee violated Government ethics rules while working at their Government duty site and also while teleworking, it increases the vulnerability that an unethical employee will misuse Government time. DCAA employs approximately 4,000 auditors, which is more than any other Federal entity. Because of DCAA's mission, organizational structure, and auditors with private for-profit businesses that telework, the risk

vulnerability has escalated. In recent years, it has become more common for DCAA auditors to telework. Combining the three factors [auditor, private for-profit business, and telework] affords an environment that allows auditors to perform tasks associated with their private for-profit businesses on Government time.

Our review covered a 6-year period, and during this period, we found that, in general, the more the subject teleworked, the less documents and e-mails associated with the subject's private for-profit tax business were transferred on to his Government computer. At the peak of the subject's teleworking – 154 days in 2008 – the subject had only one document associated with his private for-profit tax business on his Government computer. Compare this to 2006, the year that had the most documents on his government computer, 56, and only 61 days of teleworking. When the number of days teleworking began to decrease to 133 days from 2008 to 2009, the documents being transferred to the subject's Government computer associated with his private for-profit tax business began to increase, with 8 documents transferred to his government computer.

There is no reason to believe that in 2008 (when the subject had only one private for-profit business document on his Government computer) the subject stopped performing tasks associated with his private for-profit tax business while teleworking. To the contrary, the reason there was a drop in private for-profit tax business activity on the subject's Government computer between 2006-2009 was due to the subject being at home with immediate access to his personal computer, client account information, and home telephone. The subject attested to the fact that during this period, he had no reason to send his private for-profit tax business clients' documents to his official Government computer because he had immediate access to his personal computer, client account information, and home telephone while teleworking.

Recommendations, Management Comments, and Our Response

A. We recommend that the Director, Defense Contract Audit Agency:

1. Take appropriate action against the subject.

Management Comments

The Director, DCAA concurred. DCAA proposed suspending the employee without pay for a significant period and reducing his grade level. DCAA also revoked subject's telework authority for a minimum of one year.

Our Response

The Director, DCAA comments were responsive and the actions meet the intent of the recommendation. Upon final adjudication of the suspension and reduction in grade, we request that DCAA provide us the documentation supporting these actions.

2. Determine what action to take to mitigate risk vulnerability.

Management Comments

The Director, DCAA concurred. The Director sent out a memorandum to all DCAA employees reiterating DCAA ethics rules and restating his position to hold accountable individuals who break these rules. DCAA also will research the feasibility of implementing an online reporting tool for all employees to report their outside employment. Finally, DCAA will review their policies and procedures for computer and network access to determine if internal controls need to be enhanced to cover time spent out of the duty station.

Our Response

The Director, DCAA comments were responsive and the actions meet the intent of the recommendation. By September 30, 2011, we request DCAA notify us of the results of the research on the feasibility of an online reporting tool for reporting outside employment.

Finding B. Personally Identifiable Information (PII) on Government Computer

During our review, we found that the subject's Government-issued computer contained personally identifiable information belonging to 30 individuals of his private for-profit tax business, to include their social security numbers, names, home addresses, and telephone numbers. The subject forwarded this information to his Government computer via e-mail from his personal business account to have it for reference at work. This action may have exposed his clients' personal information to unauthorized recipients and placed their identity in jeopardy.

Federal Government Policy on Personally Indentifiable Information on Government Systems

Office of Management and Budget

PII and its protection became the focus of the Executive Office of the President in 2006. The President issued Executive Order 13402, Strengthening Federal Efforts to Protect Against Identity Theft, dated May 10, 2006. This order established the Identity Theft Task Force and required the task force to formulate a strategic plan. The Office of Management and Budget (OMB) also issued Memorandum 06-15, Safeguarding Personally Identifiable Information, dated May 22, 2006, directing all departments and agencies to review their policies, procedures, and controls on PII. As soon as the task force issued its strategic plan to the President on April 23, 2007, OMB issued a memorandum to all executive departments and agencies – OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, dated May 22, 2007 – directing the identification, control, and reduction of PII. It also directed the development of guidance to report breaches of PII.

Department of Defense

DOD implemented OMB M-06-15 by issuing Office of the Secretary of Defense Administration and Management Memorandum, Safeguarding Personally Identifiable Information, dated June 15, 2006, directing all Components to review their policies, procedures, and controls on PII. One year later, DOD implemented OMB M-07-16 by issuing Office of the Secretary of Defense Administration and Management Memorandum, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, dated September 21, 2007. Emphasizing DOD's serious intent to safeguard PII within the department, the Office of the Secretary of Defense Administration and Management reissued the exact same September 21, 2007 memorandum's guidance twice on September 25, 2008 and June 5, 2009. The guidance contained in these memoranda augment DOD's privacy guidance contained in DOD Directive 5400.11, DOD Privacy Program, dated May 8, 2007; and DOD 5400.11-R, Department of Defense Privacy Program, dated May 14, 2007. The DOD guidance

directs the review of PII holdings and provides incident reporting criteria if there is a breach.

Defense Contract Audit Agency

DCAA implementation of OMB's and DOD's policy on PII is contained in DCAA Instruction No. 5410.10, DCAA Privacy Program, dated February 15, 2011. This guidance specifically states:

- DCAA will collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by statute or Executive Order.
- The Chief Information Officer is responsible for ensuring that personal information in electronic form is only acquired and maintained when necessary.
- The procedures to follow in the case of actual or suspected compromise of personally identifiable information.

The mission of DCAA does not encompass the collection of private citizens' personal tax information. What was not to be foreseen in the above policies was a situation where a Federal employee would introduce private citizens' PII onto a Federal Government agency's information system, as is the case in this report. All policies focused on identifying, reducing, and where possible, eliminating PII on Government systems. The policies also focused on how to report a breach of an agency's authorized PII holdings. The subject of this review, without any authorization, improperly introduced private citizens' PII into the DCAA network.

Internal Revenue Code Concerning Disclosure of Tax Return Information

Internal Revenue Code, 26 U.S.C. §7216 (2010), Penalty for Disclosure or Use of Tax Return Information, states:

> Any person who is engaged in the business of preparing, or providing services in connection with the preparation of, returns of the tax imposed by chapter 1, or any person who for compensation prepares any such return for any other person, and who knowingly or recklessly discloses any information furnished to him for, or in connection with, the preparation of any such return, or uses any such information for any purpose other than to prepare, or assist in preparing, any such return, shall be guilty of a misdemeanor, and upon conviction thereof, shall be fined not more than $1,000, or imprisoned not more than 1 year, or both, together with the costs of prosecution. The exception where this shall not apply is if such disclosure is made pursuant to any other provision of this title or pursuant to an order of the court.

Internal Revenue Code, 26 U.S.C. §6713 (2010), Disclosure or Use of Information by Preparers of Returns, states:

> If any person who is engaged in the business of preparing, or providing services in connection with the preparation of, returns of tax imposed by chapter 1, or any person who for compensation prepares any such return for any other person, and who discloses any information furnished to him for, or in connection with, the preparation of any such return, or uses any such information for any purpose other than to prepare, or assist in preparing, any such return shall pay a penalty of $250 for each such disclosure or use, but the total amount imposed under this subsection on such a person for any calendar year shall not exceed $10,000. The exception where this shall not apply is if such disclosure is made pursuant to any other provision of this title or pursuant to an order of the court.

Although the subject of this report did not disclose taxpayer information to a specific individual, the subject's actions in forwarding his clients' tax information to his official Government computer via e-mail may be considered reckless disclosure. This review obtained access to the confidential taxpayer information, and DCAA information technology personnel could have come across this confidential information since all e-mails are controlled by DCAA network administrators.

State Board of Public Accountancy Rules of Professional Conduct

State Board of Accountancy Rules of Professional Conduct, Chapter 30-X-6-.04, Responsibilities to Clients, states:

> A registrant shall not disclose any confidential information obtained in the course of a professional engagement except with the consent of the client.

Although the subject of this report did not disclose his clients' information to a specific individual, the fact that the subject transferred this confidential information to his Government computer exposed the sensitive information to Government officials conducting the official investigation, and possibly to DCAA information technology personnel with access to e-mails on the DCAA network. The subject is licensed by a specific State's Board of Public Accountancy.

American Institute of Certified Public Accountants Code of Professional Conduct

American Institute of Certified Public Accountants Code of Professional Conduct, ET Section 301 – Confidential Client Information, Subsection .01 Rule 301 – Confidential Client Information states:

> A member in public practice shall not disclose any confidential client information without the specific consent of the client.

Although the subject of this report did not disclose his clients' information to a specific individual, the fact that the subject transferred this confidential information to his Government computer exposed the sensitive information to Government officials conducting the official investigation, and possibly to DCAA information technology personnel who have access to e-mails on the DCAA network. The subject is a Certified Public Accountant and a member of the American Institute of Certified Public Accountants.

Subject's Sworn Statement Concerning Personally Identifiable Information on His Government-Issued Computer

We questioned the subject about the PII we found on his Government-issued computer. We specifically mentioned 31 names, showing the subject the actual documents containing the social security numbers, names, home addresses, and telephone numbers of private citizens who were clients of the subject's private for-profit tax business. These documents consisted of:

- Letters.
- IRS Forms W-2, W-4, 1040 (with Schedules), 1099, 4868, 8812, and 8863.
- State Income Tax forms.
- E-Trade Financial stockbroker statements.
- Weekly employee pay stubs.

When shown the actual documents, the subject acknowledged all of the documents but one. In the document not acknowledged, the subject stated that the identification number was not a social security number, but rather a Federal Employer Identification Number for a business. When asked why these documents were on his Government-issued computer, the subject stated that he forwarded them via e-mail to his Government computer so he could have the documents available for reference at work while talking to a client, a lawyer, or a State revenue office on the phone. The subject acknowledged that his actions constituted misuse of Government time and equipment. Further, the subject acknowledged the document showing that he had received annual training on the authorized use of his Government-issued computer, and stated that he understood that PII was not authorized to be on his Government-issued computer.

Recommendations, Management Comments, and Our Response

B. We recommend that the Director, Defense Contract Audit Agency:

1. Contact the U.S. Department of the Treasury to determine:

a. whether any Federal laws or regulations have been violated; and

b. whether the affected taxpayers are required to be contacted concerning this breach.

Management Comments

The Director, DCAA concurred. DCAA will forward a copy of this report with the subject's identifying data to the U.S. Department of the Treasury Inspector General's office for action.

Our Response

The Director, DCAA comments were responsive and the actions meet the intent of the recommendation. We request that DCAA include us as a courtesy copy addressee on the transmittal letter.

2. Contact the specific State Board of Public Accountancy to determine whether any State laws or rules have been violated.

Management Comments

The Director, DCAA concurred. DCAA will forward a copy of this report with the subject's identifying data to the applicable State(s) Board of Public Accountancy for action.

Our Response

The Director, DCAA comments were responsive and the actions meet the intent of the recommendation. We request that DCAA include us as a courtesy copy addressee on the transmittal letter.

3. Contact the American Institute of Certified Public Accountants to determine whether any rules have been violated.

Management Comments

The Director, DCAA concurred. DCAA will forward a copy of this report with the subject's identifying data to the American Institute of Certified Public Accountants for action.

Our Response

The Director, DCAA comments were responsive and the actions meet the intent of the recommendation. We request that DCAA include us as a courtesy copy addressee on the transmittal letter.

4. Take appropriate action against the subject.

Management Comments

The Director, DCAA concurred. DCAA proposed suspending the employee without pay for a significant period and reducing his grade level. DCAA also revoked subject's telework authority for a minimum of one year.

Our Response

The Director, DCAA comments were responsive and the actions meet the intent of the recommendation. Upon final adjudication of the suspension and reduction in grade, we request that DCAA provide us the documentation supporting these actions.

5. Have the DCAA Chief Information Officer:

a. Determine how to mitigate risk of unauthorized personally identifiable information being transmitted onto, or from, DCAA's information systems network(s).

b. Determine how to purge all of the subject's e-mails, e-mail attachments, and documents containing unauthorized personally identifiable information from DCAA systems and his Government-issued computer.

c. Determine whether a breach notification to the United States Computer Emergency Readiness Team is required.

d. Determine whether a breach notification to affected individuals is required.

Management Comments

The Director, DCAA concurred with Recommendations 5a through 5d. The DCAA Chief Information Officer ordered research to ensure that DCAA is using the most current, available methods to mitigate risk of unauthorized PII being transmitted onto or from its information systems, such as logical access control, encryption of data, and training. The Chief Information Officer further stated that DCAA continually re-evaluates their system controls as additional tools become available. The Chief Information Officer confirmed that all the unauthorized PII has been removed. Finally, the Chief Information Officer applied applicable policies to determine if a breach had occurred at DCAA, and if so, did it need to be reported, and did the affected individuals need to be notified. The Chief Information Officer determined that a breach did not occur, and therefore, United States Computer Emergency Readiness Team and affected individuals did not need to be notified by DCAA.

Our Response

The Director, DCAA comments were responsive and the actions meet the intent of the recommendations.

Finding C. Unauthorized Software on Government Computer

During our review, we found unauthorized software on the subject's Government computer – specifically, five games. The subject was able to maintain these games on his Government computer because the games were embedded in Microsoft Excel spreadsheets. Having and playing games on a Government computer is unauthorized, a waste of taxpayers' dollars, and can expose the network to malware/viruses.

DCAA Policy on Unauthorized Software on Government Computers

DCAA policy does not permit unauthorized software on its computers. DCAA Regulation No. 8500.1, Information Assurance (IA) Program, dated September 24, 2009, specifically states that no user will introduce or use unauthorized software on the DCAA information system. DCAA Rules for Computer Users [Enclosure 4 to DCAAR No. 8500.1], which users are required to read and certify annually, states:

- Do not introduce or use unauthorized software, firmware, or hardware onto the system or enclave.
- Users must not play computer games.

Subject's Sworn Statement Concerning Games on His Government Computer

During our interview of the subject, he acknowledged the five games we found on his computer. We asked the subject how these games became embedded in a Microsoft Excel file, and whether this was done to circumvent information technology rules forbidding unauthorized software on Government computers. The subject stated that he did not know how the games were embedded into a Microsoft Excel file, and that he received these games via e-mail from someone many years ago. The subject agreed that the games were embedded most likely to get around computer security rules. When shown a copy of his electronically-signed annual computer use training and certification, he acknowledged receiving the annual training and admitted to knowing that games were not authorized to be on his Government-issued computer.

Recommendations, Management Comments, and Our Response

C. We recommend that the Director, Defense Contract Audit Agency:

1. take appropriate action against the subject; and

Management Comments

The Director, DCAA concurred. DCAA proposed suspending the employee without pay for a significant period and reducing his grade level. DCAA also revoked subject's telework authority for a minimum of one year.

Our Response

The Director, DCAA comments were responsive and the actions meet the intent of the recommendation. Upon final adjudication of the suspension and reduction in grade, we request that DCAA provide us the documentation supporting these actions.

2. have the DCAA Chief Information Officer determine how to mitigate risk of employees having unauthorized software (e.g., games) on their Government computers.

Management Comments

The Director, DCAA concurred. The DCAA Chief Information Officer ordered a review of the current internal controls in place and will continue to evaluate changing technology in the future.

Our Response

The Director, DCAA comments are responsive and the actions meet the intent of the recommendation.

Appendix. Scope and Methodology

We reviewed the Defense Hotline complaint to determine whether we could substantiate the allegation. Our review covered the period 2005 through 2010. As part of our review, we:

- seized the subject's Government computer and analyzed its contents (which included searching the entire hard drive for Microsoft Word and Microsoft Excel files; Adobe PDF files; e-mails in the current Microsoft Outlook Inbox and Saved Mail.pst, Archive.pst; Microsoft Outlook calendars; and installed software);
- interviewed the subject's current and past supervisors;
- interviewed a DCAA Regional Director;
- interviewed and recorded the subject under oath;
- reviewed applicable laws, policies, and regulations pertaining to the misuse of Government time and equipment, personally identifiable information, and unauthorized software on a Government computer;
- reviewed the subject's Official Personnel File maintained by the Defense Finance and Accounting Service;
- reviewed the subject's annual Confidential Financial Disclosure Reports; and
- reviewed the subject's certifications of annual training in ethics, privacy, and information assurance (authorized Government computer use).

We performed this review from October 2010 through March 2011. The review was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation.

Use of Computer-Processed Data

We did not rely on computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, no prior coverage has been conducted on a Federal employee using Government time and equipment to perform tasks associated with a private for-profit business or unauthorized software on a Government computer. However, the Government Accountability Office (GAO) has issued 4 reports during the last 5 years discussing personally identifiable information. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov.

GAO

GAO Report No. GAO-09-759T, "Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, But Vulnerabilities Remain," June 17, 2009

GAO Report No. GAO-08-795T, “Privacy: Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information,” June 18, 2008

GAO Report No. GAO-08-536, “Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information,” May 19, 2008

GAO Report No. GAO-08-343, “Information Security: Protecting Personally Identifiable Information,” January 25, 2008

Defense Contract Audit Agency Management Comments

DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

OFFICE OF THE DIRECTOR

June 21, 2011

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR POLICY AND OVERSIGHT, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Response to Department of Defense Inspector General (DODIG) Draft Report on a Hotline Complaint Regarding a Defense Contract Audit Agency Employee Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment (Project No. D2010-DIP0AI-0253.000)

Thank you for the opportunity to respond to the subject draft report.

We agree with the DODIG findings in the draft report that the DCAA employee was (1) conducting activities associated with his private for-profit tax business on Government time and using Government equipment, (2) had unauthorized personally identifiable information on his computer, and (3) had unauthorized software on his computer.

DODIG Recommendations.

A. Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment

A.1 Take appropriate action against the subject.

DCAA Response. Concur. On June 9, 2011, DCAA proposed suspending the employee without pay for a significant period and reducing his grade level. In addition, the employee is restricted from telework for a period of one year, at which time his supervisor will revisit the restriction decision.

A.2 Determine what action to take to mitigate risk vulnerability.

DCAA Response. Concur. We agree intellectually that an unethical employee can take advantage of the inherent risk of the work environment, but the issue is the employee's unethical behavior, not teleworking. We agree that by September 30, 2011, we will review our policies and procedures related to computer and network access, and related to employee time spent out of the duty station to determine if related internal controls can be strengthened. Additionally, the Director issued a memorandum on May 16, 2011 reiterating DCAA ethics rules and restating his position to hold accountable individuals who break these rules. DCAA is also researching the feasibility of implementing an online

June 21, 2011

SUBJECT: Response to Department of Defense Inspector General (DoDIG) Draft Report on a Hotline Complaint Regarding a Defense Contract Audit Agency Employee Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment (Project No. D2010-DIP0AI-0253.000)

reporting tool for all employees to report their outside employment. Estimated completion date for this research is September 30, 2011.

B. Personally Identifiable Information (PII) on Government Computer

B.1 Contact the U.S. Department of the Treasury to determine:

a. whether any Federal laws or regulations have been violated; and
b. whether the affected taxpayers are required to be contacted concerning this breach.

DCAA Response. Concur. Within 30 days of this report being published, DCAA will forward the report, along with identifying data, to the responsible U.S. Department of the Treasury Inspector General's office.

B.2 Contact the specific State Board of Public Accountancy to determine whether any State laws or rules have been violated.

DCAA Response. Concur. Within 30 days of this report being published, DCAA will forward the report, along with identifying data, to the applicable state licensing board.

B.3 Contact the American Institute of Certified Public Accountants to determine whether any rules have been violated.

DCAA Response. Concur. Within 30 days of this report being published, DCAA will forward the report, along with identifying data, to the AICPA.

B.4 Take appropriate action against the subject.

DCAA Response. Concur. On June 9, 2011, DCAA proposed suspending the employee without pay for a significant period and reducing his grade level. In addition, the employee is restricted from telework for a period of one year, at which time his supervisor will revisit the restriction decision.

B.5a Have the DCAA Chief Information Officer determine how to mitigate risk of unauthorized personally identifiable information being transmitted onto, or from, DCAA's information system network(s).

DCAA Response. Concur. This action is complete. The nature of auditing requires some authorized PII information to be available on many of the Agency computers, so we are not able to use methods that preclude any PII. Upon receipt of this report, we researched available methods used in this area and verified that DCAA currently uses a number of

June 21, 2011

SUBJECT: Response to Department of Defense Inspector General (DoDIG) Draft Report on a Hotline Complaint Regarding a Defense Contract Audit Agency Employee Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment (Project No. D2010-DIP0A1-0253.000)

methods to mitigate the risk of unauthorized personally identifiable information being transmitted onto or from its information systems. DCAA requires all users of its information systems to take annual training on the handling of privacy information and Information Assurance. In addition, DCAA deploys technical methods such as logical access controls and strong encryption of data to ensure data can only be accessed by those with a need to know. We will continually re-evaluate our system controls as additional tools become available.

B.5b Have the DCAA Chief Information Officer determine how to purge all of the subject's e-mails, e-mail attachments, and documents containing unauthorized personally identifiable information from DCAA systems and his Government-issued computer.

DCAA Response. Concur. This action is complete. Upon receipt of this draft report, DCAA conducted an analysis of all network drive share (folders), e-mail server accounts, e-mail server backup tapes, and laptop hard drives associated with the subject of this case. All unauthorized personally identifiable information has been removed.

B.5c Have the DCAA Chief Information Officer determine whether a breach notification to the United States Computer Emergency Readiness Team is required.

DCAA Response. Concur. This action is complete. We determined that the introduction of PII from the subject's clients to his DCAA laptop does not constitute a PII violation. Compromised PII is defined by the Defense Privacy and Civil Liberties Office as the government's loss of control, breach, unauthorized disclosure, unauthorized acquisition, or unauthorized access. In this case, the subject, acting in his private/non-official capacity, was provided PII information voluntarily by his clients; therefore, his access was authorized by his clients. There is no evidence that DCAA personnel, other than those authorized to conduct this investigation, had access to these records or that the records were introduced to any DCAA network systems. Based upon this information and conversations with the Defense Privacy and Civil Liberties Office, no PII breach has occurred and there is no need to notify the United States Computer Emergency Readiness Team, the Defense Privacy and Civil Liberties Office, or the subject's clients.

B.5d Have the DCAA Chief Information Officer determine whether a breach notification to affected individuals is required.

DCAA Response. Concur. This action is complete. As discussed in our response to B.5c above, we determined that no PII breach occurred and therefore no notification to the subject's clients is required.

June 21, 2011

SUBJECT: Response to Department of Defense Inspector General (DoDIG) Draft Report on a Hotline Complaint Regarding a Defense Contract Audit Agency Employee Conducting Private For-Profit Tax Business Activity on Government Time and Using Government Equipment (Project No. D2010-DIP0AI-0253.000)

C. Unauthorized Software on Government Computer

C.1 Take appropriate action against the subject.

DCAA Response. Concur. On June 9, 2011, DCAA proposed suspending the employee without pay for a significant period and reducing his grade level. In addition, the employee is restricted from telework for a period of one year, at which time his supervisor will revisit the restriction decision.

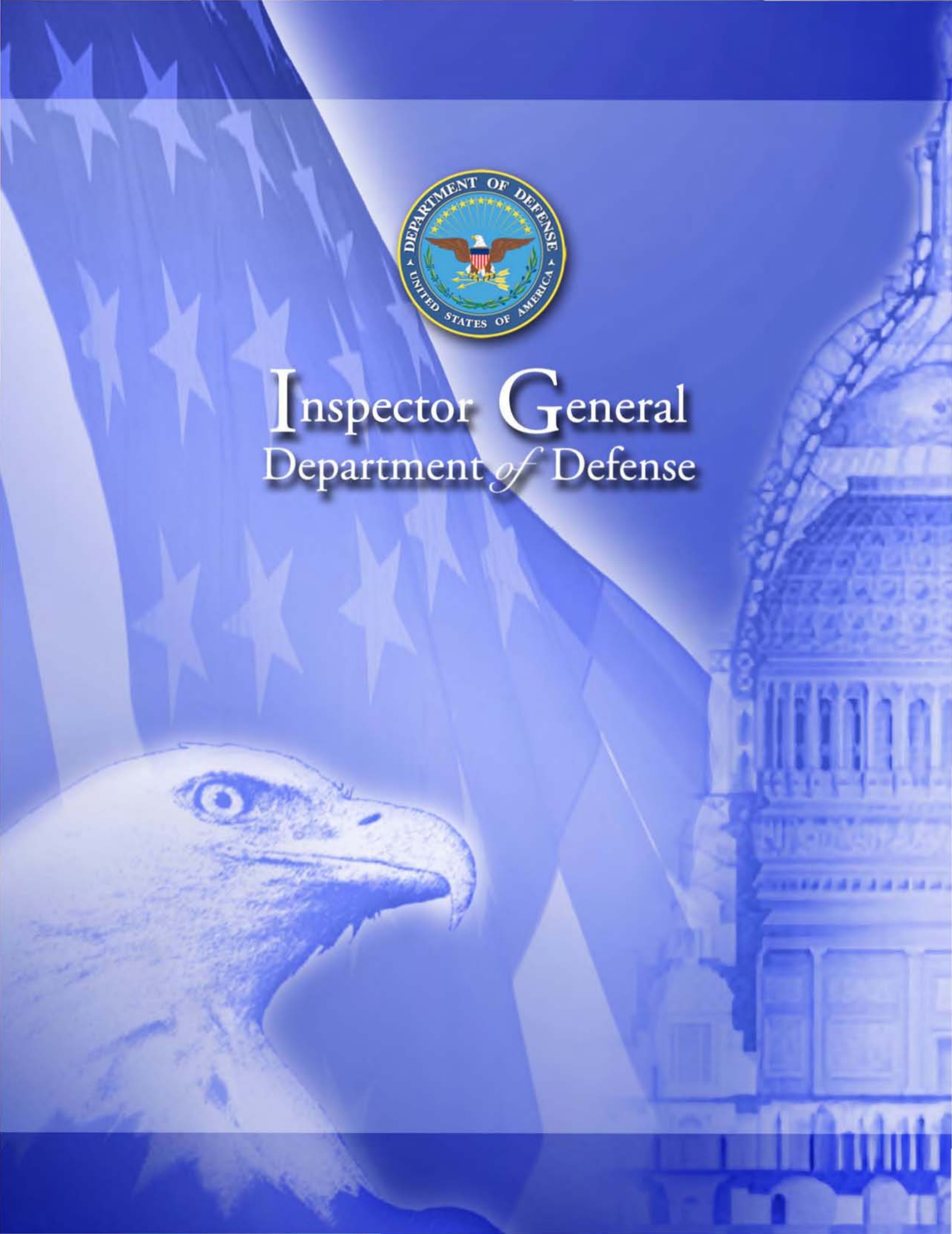
C.2 Have the DCAA Chief Information Officer determine how to mitigate risk of employees having unauthorized software (e.g., games) on their Government computers.

DCAA Response. Concur. This action is complete. Upon receipt of this draft report, we evaluated the DCAA internal controls in place to address this issue and will continue to evaluate changing technology in the future.

Please direct any questions or concerns to the undersigned at (703) 767-3200.

Patrick J. Fitzgerald
Director

4



Inspector General
Department of Defense